



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,291	04/16/2004	Catherine Helen Gebotys	1679-14/EDEV	7948
89298	7590	11/25/2009		
Dimock Stratton LLP/Research In Motion Limited 20 Queen Street West, 32nd Floor, Box 102 Toronto, ON M5H 3R3 CANADA			EXAMINER TRUONG, THANHNGA B	
			ART UNIT 2438	PAPER NUMBER
			NOTIFICATION DATE 11/25/2009	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rim-uspto@dimock.com
portfolioprossecution@rim.com
lforster@dimock.com

Office Action Summary	Application No. 10/825,291	Applicant(s) GEBOTYS, CATHERINE HELEN	
	Examiner THANHNGA B. TRUONG	Art Unit 2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10/21/09 (RCE).
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 9-13 and 30-34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☐ Claim(s) _____ is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 21, 2009 has been entered. Claims 1-58 are pending. Claims 1-8, 14-29, and 35-58 are cancelled by the applicant. At this time, claims 9-13 and 30-34 are still rejected.

Response to Arguments

2. Applicant's arguments with respect to claims 9-13 and 30-34 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments filed October 21, 2009 with respect to claims 1-8, 14-29, and 35-58 have been fully considered but they are not persuasive. Based on the application's record, especially claims that file on August 29, 2008, applicant has agreed to cancel these claims 1-8, 14-29, and 35-58. However, claims status filed on October 21, 2009 with respect to claims 1-8, 14-29, and 35-58 have shown with "withdrawn" status. Examiner presumed that this may have been inadvertently overlooked by the applicant. Appropriate correction is required with the next response.

Claim Objections

3. Claims 1-8, 14-29, and 35-58 are objected to because of the following informalities: Based on the application's record, especially claims that file on August 29, 2008, applicant has agreed to cancel these claims 1-8, 14-29, and 35-58. However, claims status filed on October 21, 2009 with respect to claims 1-8, 14-29, and 35-58 have shown with "withdrawn" status. Examiner presumed that this may have been inadvertently overlooked by the applicant. Appropriate correction is required by the applicant with the next response.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. § 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 9-13 and 30-34 are rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

As to independent claims 9 and 12, while the claim recites a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. § 101 must (1) be tied to a particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. *See page 10 of In Re Bilski 88 USPQ2d 1385.* Specifically, claim 14 recites "the tag authentication method comprising: classifying information... finding a group... finding a tag's secret information", but nowhere in the claim does it state what particular apparatus does (or is positively tied with) these series of steps. Because the instant claim is neither positively tied to a particular machine that accomplishes the claimed method steps nor transforms underlying subject matter of the claim to a different state or thing, the claim therefore does not qualify as a statutory process under 35 U.S.C. § 101.

As to dependent claims 10-11 and 13, they are rejected under 35 U.S.C. § 101 for depending upon the non-statutory subject matter recited by independent claims 9 and 12 respectively.

As to independent claim 30 and 33, these claims recite "the computing device program product for improving the resistance...", however in the specification, page 10, lines 1-4 of paragraph 43, Applicant has defined computer program product as

Art Unit: 2438

" *the computer program product may be embodied in, signals carried by networks, including the Internet or may be embodied in media such as magnetic, electronic or optical storage media.*)." This definition of computer program product clearly includes carrier wave mediums and propagated data signals over a network which is nonstatutory. "Carrier waves (such as data transmission through the internet)..." is not a "process, machine, manufacture, or composition of matter." Those four categories define the explicit scope and reach of subject matter patentable under 35 U.S.C. § 101; thus, such a carrier wave cannot be patentable subject matter." (In re Petrus A.C.M. Nuijten; Fed Cir, 2006-1371, 9/20/2007). Because the full scope of claims 30 and 33 as properly read in light of the disclosure encompasses non-statutory subject matter (i.e., because the limitation "computer program product" would include a non-statutory signal, carrier wave, etc.), claims 30 and 33 are rejected under 35 U.S.C. § 101 for reciting non-statutory subject matter.

As to dependent claims 31-32 and 34, they are rejected under 35 U.S.C. § 101 for depending upon the non-statutory subject matter recited by independent claims 30 and 33 respectively.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 9-13 and 30-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al (US 6,278,783 B1), and further in view of Moyse et al (US 5,446,651).

a. Referring to claim 9:

i. Kocher teaches a split-mask, masking countermeasure method for improving the resistance, to power analysis attacks, of a processing unit performing a defined cryptographic function using a key, the method comprising the following steps:

(1) obtaining the key and a random key mask value r (see Figure 1, element 100; column 8, line 65 through column 9, line 13 of Kocher);

(2) obtaining a set of n random input values $m_{\text{sub.in}1}, \dots, m_{\text{sub.in}n}$ (column 6, lines 39-45 of Kocher);

(3) defining a masked function by masking the defined cryptographic function with the value $m_{\text{sub.in}1} \wedge \dots \wedge m_{\text{sub.in}n}$ (see Figure 2, element 220; column 8, lines 31-51 of Kocher);

(4) masking the key with the random key mask value r to define the value m_{key} (see Figure 2, element 220; column 7, lines 30-33; column 8, lines 31-51 of Kocher);

(5) obtaining a set of random split mask values m_1, \dots, m_{n-1} (column 6, lines 40-55; column 7, lines 30-48 of Kocher);

(6) defining a split mask value m_n to be $r \wedge m_{\text{sub.in}1} \wedge \dots \wedge m_{\text{sub.in}n} \wedge m_1 \wedge \dots \wedge m_{n-1}$ (see Figure 2; column 7, lines 30-33; column 8, lines 31-51 of Kocher); and

(7) using the values m_1, \dots, m_n and m_{key} to define input for the masked function (see Figure 2, element 220; column 8, lines 31-51 of Kocher);

ii. Although Kocher teaches the technique of key splitting, Kocher is silent on the capability of splitting mask value. On the other hand, Moyes teaches this limitation in column 29, lines 25-39 of Moyes.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Kocher with the teaching of Moyes for improving the encryption operation within the network communication.

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Kocher with the teaching of Moyes to provide and enhance the technique of splitting mask value to secure network communication).

b. Referring to claim 10:

i. Kocher further teaches:

(1) in which the encryption function is a table look-up **(column 5, lines 7-32 of Kocher)**.

c. Referring to claim 11:

i. Kocher further teaches:

(1) in which masking is a bitwise exclusive or operation carried out on binary values **(column 2, lines 25-29 of Kocher)**.

d. Referring to claims 12-13:

i. These claims have limitations that is similar to those of claims 9-11, thus they are rejected with the same rationale applied against claims 9-11 above.

e. Referring to claims 30-32:

i. This claim consists a computing device program product for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium to implement claims 9-11 and thus they are rejected with the same rationale applied against claims 9-11 above.

f. Referring to claims 33-34:

Art Unit: 2438

i. This claim consists a computing device program product for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium to implement claims 9-11 and thus they are rejected with the same rationale applied against claims 9-11 above.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached at 571-272-3787. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/

Primary Examiner, Art Unit 2438

TBT

November 22, 2009